



DRAFT Privacy Act and Emails



Introduction

Background

Email is quite useful to FSA as a means of communication with internal and external parties. In the upcoming months email will become a critical method for communicating with account holders who are in the military. American service members are being sent overseas, where they may have limited or unreliable access to phones or to the postal service. However, they are able to correspond with FSA through email. They will likely be utilizing email as the prime method for conversing with FSA regarding their accounts.

Members within FSA have had questions regarding sending Privacy Act information over email. The purpose of this document is to review FSA's current practices of sending Privacy Act information over email and determine whether the risk of sending the data through email is appropriate and reasonable given the sensitivity of the information being transmitted.

Scope

This document focuses on the FSA sending out Privacy Act information through email, rather than on incoming emails that contain personal information. The Privacy Act applies only after a government agency receives personal information. FSA does not require that a student or group send personal information through email, that is their choice and any risk associated with sending email lies with the sender. FSA realizes there are things that could be done to protect incoming email, however FSA does not have the authority to dictate to other groups what software, etc. they must purchase before they send FSA an email.

Requirements

The nature and mission of helping students fund education make handling Privacy Act information an inevitable part of the duties of FSA. The Privacy Act requires that the Department of Education "establish appropriate administrative, technical and physical safeguard to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained," 5 U.S. 552a(e)(10). The Privacy Act does not dictate what the appropriate safeguards are for protecting information as described above, which gives FSA flexibility in implementing appropriate safeguards, but the organization should conduct a security analysis (which is represented by this document) to show how FSA exercised discretion.



DRAFT Privacy Act and Emails



Methodology

The first step in conducting a security analysis is to gain a generalized understanding of the current practices within FSA regarding distribution of Privacy Act information through emails. This will provide a basis for understanding which groups and their business processes might be affected by a change in policy and also shows a snapshot of the activities that are currently done in conjunction with Privacy Act information distribution.

FSA undertook a number of steps to gain this knowledge. The FSA SSO sent out an email to the SSOs of the various systems within FSA, requesting information on the matter. A number of the SSOs responded with information on their activities.

Next, the group selected a representative sample of ten systems for follow up action. The BearingPoint team created a list of comprehensive questions addressing all aspects of Privacy Act information and emails. The selected systems were sent the questionnaire to complete and return. BearingPoint followed up with a number of the teams and conducted meetings with the SSOs and some system managers in order to get an understanding of their practices on a more granular level. Besides the individual systems, BearingPoint gathered information from the legal department within Department of Education, which provided a better understanding of the Department's interpretation of Privacy Act requirements. Current policies and procedures were also reviewed. The information from the ten systems was compiled into a spreadsheet to facilitate the analysis portion of the risk assessment.

The next section of the document will delve into the risk assessment portion. First, the current practices, collected from our research, are discussed. Then the threats, vulnerabilities, impact and likelihood will be reviewed. These components are the basis of final risk determination.

Current practices

When focusing on the current practices the most important questions consisted of discovering how much Privacy Act information was actually being distributed, who it was being sent to, and the practices surrounding the transmissions. Of the ten systems that were analyzed, only two of the systems used email to transmit Privacy Act data and only in response to inquiries from other parties; the main parties include other Department of Education employees, contractors, students, schools, debt collection, and loan agencies. Other systems use other methods to handle inquiries; the majority of FSA responses are made by sending letters through the mail or calling the person back on the phone. Some systems refer to the inquirer to a help desk where they can gain more information. One system refers the students to an encrypted link where they use their password to obtain more information. One of the systems that send out Privacy Act information through email uses an encrypted link, to provide additional protection to the email.



DRAFT Privacy Act and Emails



Threats and Vulnerabilities

Sending information through email does have some associated risks. The biggest possible problem would be that someone other than the intended recipient would receive the email that contains the personal information. The threats and vulnerabilities associated with email transmission relate back to the issue of the correct recipient.

Threats

One of the biggest threats to email transmission is the ability of another party to intercept an email. This attack is known as a “man-in-the-middle” attack, where a party intercepts the email message while it is in transit. One potential problem would be that the information, after interception, is stolen outright and the addressee never receives the email. Another possibility is that the message could be captured and the contents altered and then passed on to the original recipient.

Vulnerabilities

Another concern with email is the identification of the recipient. Is the person who is sending the message really the person whose account the message is coming from? FSA does not want to send out information to a person, only to later discover that the person at the other end was not the same person listed on the email account.

Also, typographical mistakes are a potential vulnerability. Accidentally typing the incorrect address could cause a message to go to the wrong person.

Likelihood

While there are threats and vulnerabilities associated with email, the overall risk of using email to transmit Privacy Act information is low. The likelihood that an attacker would actually perform a “man-in-the-middle” attack is low. The volume of daily email transmissions is so high in general that the chances of an email from FSA being intercepted would be minimal, and to narrow it down to the chances of intercepting an FSA email with Privacy Act information is minute. Problems regarding typographical errors are usually avoided by the FSA employee hitting the reply button to respond to an email, as opposed to retyping the email address.

Conclusion

The usage of email to transmit personal information remains a viable and important method for communication. FSA encourages systems to use other ways, if possible, to respond to parties where Privacy Act information is involved. FSA inquiries show that the overall usage of email to transmit Privacy Act information is low. There are risks associated with using email, however these risks are negligible and do not overcome the usefulness of email.